SUPPLIER SHIELD

Information Security Charter

Rue de la gare 39 | 1110 Morges | Switzerland | T +41 21 802 35 54 | request@suppliershield.com
https://www.suppliershield.com/

Table of Contents

1. Purpose

This Charter outlines Supplier Shield™ objectives and the structure of the Information Security Management System. It is intended for external audiences requiring visibility in our ISMS Framework. While the governance framework, responsibilities, and commitment required to protect the confidentiality, integrity, and availability of our assets are presented, Supplier Shield™ reserves the right to omit confidential information that may compromise the employees, stakeholders or company's security and privacy.

Supplier Shield™ has developed an ISMS structured with a risk-based approach to managing information security and privacy across the organization and protect its information, resources, and systems.

This Charter promotes alignment with industry best practices and ISO/IEC 27001:2022 through the integration of principles such as zero-trust architecture, privacy by design, privacy by default, and the CIS Security Benchmarks. The Charter guarantees uniform implementation of security policies, controls, and awareness measures across all business functions.

The Charter also defines the specific responsibilities supporting the effective implementation, operation, and continual improvement of the ISMS across the organization.

2. Scope

This Charter apply to all Supplier Shield™ personnel, processes, systems, and third-party providers that access, manage, store, or transmit Supplier Shield™ data or support its infrastructure.

The Charter encompasses:

- Supporting systems, including applications, databases, and cloud environments.
- Personnel, including employees, contractors, and key third-party partners.
- Processes, procedures, and other relevant documented information that contribute to the protection of information assets.

3. Definitions

Term / Abbreviation	Definition
Availability	Characteristic of the information by which authorized persons can access it when it is needed.
Confidentiality	Characteristic of the information by which it is available only to authorized persons or systems.
Cryptography	Discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized use.
Information Security Management System (ISMS)	System to manage risks related to the security of information an organization own or handle.
Integrity	Characteristic of the information by which it is changed only by authorized persons or systems in an allowed way.
Steering Committee (SteerCo)	Information Security Steering Committee responsible for overseeing the effective implementation of the ISMS, and ensuring that the confidentiality, integrity, and availability of Supplier Shield™ systems and data are maintained.
Threat	Potential cause of an unwanted incident, which can result in harm to a system or organization.
Vulnerability	Weaknesses of an asset or control that can be exploited so that an event with a negative consequence occurs.

4. Roles & Responsibilities

Steering Committee (SteerCo)

- Governs and oversees the ISMS, ensuring alignment with enterprise risk management and business objectives.
- Ensures regulatory and customer requirements are reflected in security and privacy activities.
- Promotes collaboration among Security, Compliance, Privacy, and IT functions.
- Reviews ISMS performance, risks, and improvement opportunities, and reports outcomes to executive management.

Chief Executive Officer (CEO)

- Aligns the ISMS with corporate objectives and regulatory requirements.
- Embeds security principles across operations, infrastructure, and product development.
- Defines and maintains the overall information security strategy and governance framework.

Product Development Director

- Integrates security and privacy requirements throughout the product lifecycle.
- Reviews major product initiatives to assess and mitigate security risks.
- Reports on control maturity and advises on secure technology adoption and improvement opportunities.

ISMS Manager

- Leads governance, risk, and compliance activities under the ISMS in line with ISO/IEC 27001.
- Oversees risk assessments, policy management, and internal audit processes.
- Monitors ISMS performance and drives continual improvement.

Legal Expert

- Ensures compliance with data protection and privacy obligations.
- Represents legal and privacy interests within the Steering Committee.

Information Security Officer (ISO)

- Embeds security within corporate IT networks, systems, and infrastructure.
- Manages technical controls, access management, and ongoing security operations.
- Provides expertise to enhance Supplier Shield™'s corporate security posture.

5. Information Security Management System Controls

a. Organizational Controls

- Governance, policies, and standards are defined, approved, and maintained to ensure consistent information security management across the organization
- An inventory of information assets is maintained, and ownership is assigned to ensure accountability. Assets are classified and handled according to their sensitivity and applicable policies.
- Major technology and business initiatives are reviewed to ensure alignment with security and compliance requirements.
- Information security risks are identified, assessed, and treated through a structured risk management process.
- The effectiveness of security controls is monitored through internal reviews and performance indicators.

b. People Controls

- Background verification is performed prior to employment where legally permissible.
- All personnel receive information security and privacy training appropriate to their role. Ongoing awareness campaigns promote a security-first culture and reinforce accountability for information protection.
- Confidentiality and non-disclosure requirements are established for employees, contractors, and third-party providers and are formalized through employment agreements or contractual clauses.

c. Physical Controls

- Office facilities and information processing areas are protected against unauthorized access, damage, and interference.
- Physical entry controls and visitor management procedures are implemented at all locations.
- Environmental safeguards (e.g., power, fire, and flood protection) are maintained to ensure operational continuity.

d. Technological Controls

- Cloud environments are managed according to defined security and privacy requirements, including access control, encryption, and continuous monitoring.
- Vulnerabilities are identified, assessed, and remediated through regular scanning, patching, and penetration testing.
- Secure development practices are integrated into the product lifecycle to prevent and mitigate security weaknesses in software and systems.
- Security testing, including vulnerability assessments and penetration tests, is performed regularly to evaluate and improve resilience.
- Cryptographic controls are applied to protect data confidentiality and integrity, with secure key management in place.

6. Document Control

a. Approval

This version is validated as of 01.11.2025 and supersedes all previous versions. For further information, please contact us via email: request@suppliershield.ch.

Title	**Information Security Charter**
Approved By	Alexis Hirschhorn
Date of Approval	01.10.2025
Version Number	1.2

b. Version History

Version	Date	Reason for Amendment
1.0	02.09.2023	Initial version
1.1	05.10.2024	Quality review and updates
1.2	01.10.2025	Review and update purpose, scope, roles & responsibilities, ISMS controls